

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT**

I, Bradley C. Smith, Special Agent, Federal Bureau of Investigation, being duly sworn,  
state:

**INTRODUCTION**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of drive data of a blue Tesla Model 3, Georgia license plate CVF5476, which is a Hertz rental car used by subject Fengyun SHI while he was visiting the Hampton Roads area on January 5-6, 2024. (the “**SUBJECT VEHICLE**”), described more fully in Attachment A. The **SUBJECT VEHICLE** is currently located at the Hertz maintenance facility located at 3323 North Military Highway in Norfolk, Virginia, 23518, within the Eastern District of Virginia. There is probable cause to believe that the electronically stored information, or drive data, as described in Attachment B, will be located in/on the **SUBJECT VEHICLE**, and is evidence, fruits, and instrumentalities of violations of 18 U.S.C §§ 795 and 796. This request for a search warrant originates from an investigation into the subject, Fengyun SHI’s, use of a cellular phone operated drone to record and photograph Huntington Ingalls Shipbuilding and BAE Systems Shipyard, both in the Hampton Roads, Virginia area. The **SUBJECT VEHICLE** is the rental car used by SHI to drive to and around the aforementioned areas.

2. This affidavit is submitted for the limited purpose of securing a search warrant. I have not included every fact known to me concerning this investigation. Instead, I have set forth only the facts necessary to establish probable cause that violations of the federal laws identified above have occurred, and that evidence, fruits, and instrumentalities of these violations are located at or on the **SUBJECT VEHICLE**. I have based my statements in this affidavit on my training and experience, personal knowledge of the facts and circumstances obtained through my participation in this investigation, information provided by the victim company, information provided by other agents and law enforcement officers, and information provided by records and databases.

### **AFFIANT BACKGROUND**

3. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation (“FBI”) assigned to the Norfolk Field Office in Chesapeake, Virginia. I have been a Special Agent with the FBI since January 2018, and currently conduct counterintelligence and counterespionage investigations. Prior to becoming a Special Agent, I worked as a Staff Operations Specialist at FBI Headquarters in Washington, DC, assigned to the Counterintelligence Division. I have received training in criminal and national security investigations at the FBI Academy in Quantico, Virginia. Additionally, I have a Juris Doctor degree from William & Mary Law School in Williamsburg, Virginia. In the course of my duties, I am responsible for investigating individuals suspected of the unlawful retention or disclosure of sensitive and classified government information, and as a result of my training and experience, I am familiar with how such offenses are committed, the relevant criminal statutes, and how foreign intelligence services recruit and handle individuals engaged in espionage activities. I have executed arrest and search warrants in previous cases.

### **APPLICABLE STATUTES**

#### **Prohibited Conduct Under the Espionage Act**

4. Title 18, United States Code, Sections 795 & 796, are part of the Espionage Act, 18 U.S.C. § 792 *et seq.*, and prohibit (among other things) taking pictures of companies that manufacture classified military equipment.

5. More specifically, 18 U.S.C. § 795 (i) authorizes the President of the United States to define certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto and (ii) prohibits, in the interest of national defense, the making of any photograph, sketch, picture, drawing, map or graphical representation of such vital military or naval installations or equipment without first obtaining

requisite permissions (e.g., from the commanding officer of the military or naval post).

6. Section 796 prohibits an individual from using an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment.

7. In Executive Order 10104, then-President Truman-in the interests of the national defense-identified vital military and naval installations and equipment requiring the protection afforded by 18 U.S.C. §§ 795 & 796. Among other vital installations and equipment, the Executive Order specifies that “[a]ny commercial establishment engaged in the development or manufacture of classified military or naval arms, munitions, equipment, designs, ships, aircraft, or vessels for the United States Army, Navy or Air Force,” falls under the protection afforded by 18 U.S.C. §§ 795 & 796. *See* Executive Order 10104. The Executive Order also specifies that “[a]ny military, naval, or air-force reservation, post, arsenal, proving ground, range, mine field, camp, base, airfield, fort, yard, station, district, or area” classified as “top secret, secret, confidential, or restricted” falls under the protection afforded by 18 U.S.C. §§ 795 & 796. *See* Executive Order 10104.

8. Both 18 U.S.C. §§ 795 and 796 are criminal offenses punishable by up to one year imprisonment.

**INFORMATION ABOUT THE EVIDENCE LIKELY TO BE FOUND ON THE  
SUBJECT VEHICLE BASED ON MY TRAINING AND EXPERIENCE AND THE  
FEATURES OF THE SUBJECT VEHICLE**

9. Based on my training, experience, and research, I know that the **SUBJECT VEHICLE**, a Tesla Model 3, has onboard computers and systems that allow it to retain data about the vehicle’s use, including location data, if and when a passenger is present, and any connected devices such as the driver’s phone. The **SUBJECT VEHICLE** was used by SHI to drive around the Hampton Roads area on January 5 and 6, 2024. In my training and experience, examining drive data stored in/on vehicles of this type can uncover, among other things,

evidence that reveals or suggests who operated the vehicle, any co-conspirators or individuals involved in the criminal activity, and location data that would show the vehicle's presence at near BAE, Huntington Ingalls, or any other site of interest and the time at such location.

**FACTS SUPPORTING PROBABLE CAUSE THAT THE SUBJECT VEHICLE IS**

**EVIDENCE OF A CRIME**

10. On January 6, 2024, at approximately 1222 hours, a Naval Criminal Investigative Service ("NCIS") Special Agent (the "SA") received information from a source at Huntington Ingalls Industries ("HII") that a Chinese Foreign Student Visa holder was operating a drone outside the 65th Street and Huntington Avenue entrance, when it became stuck in a tree at a local residence. As background, HII is the only U.S. manufacturer of U.S. Navy carriers and manufactures and houses U.S. Navy submarines. The **SUBJECT VEHICLE** operator, Fengyun SHI (1010 Jefferson Commons Circle, Unit \*\*\*\*, Saint Paul MN, DOB: \*\*/\*\*/1998, driving rental car Georgia License plate # CVF5476), left the drone, which is an unmanned aircraft system equipped with a camera for observing and recording video while in flight, in the tree. Newport News Police Department ("NNPD") responded and provided aforementioned information to the HII security source. A database check on SHI showed SHI, Fengyun, FI Visa; Academic or Language Student; DOB: \*\*/\*\*/1998; Advanced Passenger Record; 07/09/2023; A392-CBP-Chicago, O'Hare Airport, Departure Location Tokyo, Japan, Chinese Passport # E71243174; F1 Academic or Language Student; initial entry on 8-11-2021, most recent 7-9-2023.

11. On January 8, 2024, the SA responded to the Huntington Avenue residence and interviewed the residence owner, ("RESIDENT"), who recovered the drone on his property. RESIDENT advised that on the morning of January 6, 2024, at approximately 1030 hours, he exited his residence to go to the store, when he encountered his neighbor across the street talking to a male subject. RESIDENT said the SUBJECT, later identified as Fengyun SHI, walked across the street and stated he needed help, and pointed to a tree on RESIDENT's property advising his drone was stuck. RESIDENT asked SHI where he was prior to locating the drone on

his property, and SHI motioned up the street and then showed RESIDENT his iPhone and stated GPS brought him to RESIDENT's address on Huntington Avenue. RESIDENT asked SHI where he was operating the drone and SHI motioned 50 yards across the street to the Newport News Shipyard. RESIDENT asked SHI where he was from, which SHI replied "China." RESIDENT asked if SHI "was a Chinese National," which SHI replied yes, and then motioned to his University of Minnesota sweatshirt and stated he was a student on break vacationing in the area. RESIDENT asked SHI about his Tesla vehicle, and SHI stated it was a rental car he picked up at the airport. RESIDENT stated that at that time he took pictures of SHI, his ID, and the license plate of the vehicle and called NNPD. RESIDENT relayed the foregoing information to NNPD when officers arrived. He gave them a basic outline of the events and then left the scene. RESIDENT later reported that on January 7, 2024, the drone fell out of the tree into his yard, due to wind, so he placed it into his shed for law enforcement. NNPD did not file a police report due to the drone being stuck in the tree at the time but did provide NCIS body cam footage of the interaction with SHI. I have reviewed the photos that RESIDENT took of SHI and confirmed that it appears to be SHI.

12. On January 11, 2024, the SA reviewed the NNPD body cam footage that showed SHI interacting with responding NNPD officers. Officers asked SHI what assistance he needed, for which SHI replied his drone was stuck in a tree. NNPD officers asked why SHI was flying the drone in that area and said that the weather was too dangerous to fly a drone. SHI appeared very nervous in the video and did not have any real reasons for why he was flying the drone during inclement weather. NNPD asked SHI if he knew he was flying the drone in restricted air space. SHI presented what appeared to be an iPhone, connected to the drone, and said he thought he could fly the drone in the residential area. SHI became nervous and cradled the cell phone towards his body, and stated he just needed help getting it out of the tree. NNPD officers asked SHI what he was doing in the area. SHI reported he flew in the day prior on January 5, 2024, rented a vehicle on vacation/leave from school, and took a tour of the Elizabeth Waterway. NNPD provided him a number to the Fire Department non-emergency line, advising he would

need to contact them and stay on the scene. SHI returned the rental vehicle approximately one hour after this law enforcement interaction and left Hampton Roads, VA.

13. Pursuant to a search warrant issued in the Eastern District of Virginia, 4:24-sw-5, the SD card retrieved from the drone, itself subject to search warrant 4:24-sw-4, was determined to contain photos and videos appearing to capture U.S. Naval vessels and/or vessels intended for use by the U.S. Navy that are drydocked at either of two defense contractors, Newport News Shipbuilding (NNSB) in Newport News, Virginia and/or BAE Systems shipbuilding in Norfolk, Virginia, as detailed below.

14. NNSB, a subsidiary of HII, is a DOD Cleared Defense Contractor (CDC) and is the largest military shipbuilding company in the U.S. HII is the sole company manufacturing the FORD Class United States Navy ("USN") Aircraft Carrier, which is the USN's newest generation of Aircraft Carrier. HII also manufactures and services USN nuclear submarines, and various unmanned underwater vessels ("UUV"). NNSB is (and was on January 6, 2024) actively manufacturing Ford class carrier(s) as well as Virginia Class nuclear submarines, components of which are classified. NNSB is a commercial establishment engaged in the development and manufacturing of classified military naval arms for the United States Navy.

15. Additionally, NCIS confirmed with the NNSB security manager that on January 6, 2024, the Commissioned aircraft carriers - USS John C STENNIS; Commissioned submarines - USS Boise, USS Columbus, and USS Montana were located at NNSB when the SUBJECT operated his drone. USN aircraft carriers have classified and sensitive systems throughout the carriers. The nuclear submarines present on that date also have highly classified and sensitive Navy Nuclear Propulsion Information ("NNPI") and those submarines even in the design and construction phase are sensitive and classified.

16. As a result, the information made available to me makes clear that these locations are "commercial establishment[s] engaged in the development or manufacture of classified military or naval arms, munitions, equipment, designs, ships, aircraft, or vessels for the United States Army, Navy or Air Force." EO 10104.

**TECHNICAL BACKGROUND REGARDING THE VEHICLE AND ITS  
INFOTAINMENT AND TELEMATICS SYSTEMS**

17. Based on my training and experience, as well as discussions with other experienced law enforcement officers and witnesses, I have learned that:

- a. Many modern motor vehicles are equipped with sensors, cameras,<sup>1</sup> transmitters, and electronic control units (ECUs)<sup>2</sup> to monitor and manage vehicle operations, track vehicle movement, and exchange information with other vehicles and infrastructure.<sup>3</sup> These systems also enable motor vehicles to interface with various types of mobile devices to facilitate the use of applications, including third-party navigation, wireless telephone, multimedia streaming, and the like. To perform

---

<sup>1</sup> As of 2018, the US National Highway Safety Transportation Agency requires new motor vehicles sold in the United States to have backup cameras installed by the manufacturer.

<sup>2</sup> “ECU” is a generic term applied to any embedded computer that controls one or more electrical systems within a vehicle. ECUs are typically installed in a vehicle by the original equipment manufacturer during the manufacturing process. There are many types of ECUs, and as vehicles have more features each year, the number of ECUs in each motor vehicle increases. Newer motor vehicles can integrate as many as 150 ECUs, ensuring, in theory, that each part of the motor vehicle is running properly. Some examples of common ECUs include the Engine Control Module, Transmission Control Module, Brake Control Module, and Suspension Control Module, as well as the Telematics Control Unit and Infotainment Control Unit.

<sup>3</sup> The infotainment and telematics systems in motor vehicles are not the same as “black box” recorders. Black box recorders are called event data recorders (EDRs) or crash data recorders. These black box recorders can record vehicle speed, engine speed, steering angle, throttle position, braking status, force of impact, seatbelt status, and airbag deployment. In 2006, the US National Highway Traffic Safety Administration (NHTSA) adopted regulations requiring EDRs to uniformly collect certain crash data to assist crash investigators with accident reconstruction efforts. In 2012, NHTSA proposed requiring manufacturers to install EDRs in all new cars and trucks, but in 2019, the NHTSA withdrew the proposal because automakers have voluntarily installed the devices in nearly all vehicles.



these computing functions, modern motor vehicles collect, process, and store significant volumes of data.

- b. Two commonly installed ECUs within motor vehicles are infotainment and telematics systems—sometimes referred to as the Telematics Control Unit and the Infotainment Control Unit. These systems typically retain large amounts of user data within the vehicle.
- c. A vehicle's infotainment system combines hardware and software to provide entertainment features. Many infotainment systems allow drivers and passengers to connect their handheld electronic devices to the vehicle. When connected, the driver and/or passengers may gain access to, for example, Global Positioning System (GPS) navigation, video players, music streaming, voice calling, texting, and traffic data. Many systems enable talking hands-free with Bluetooth connectivity, listening to music, watching videos, or pulling up a mapped route to a destination. Many of these features are accessible via the (usually interactive) console located on the front dashboard of the vehicle.
- d. A vehicle's telematics system typically collects and stores diagnostic data from various systems (other ECUs) within the vehicle, including historical navigation points, speed, and event data. Historical event data may include information regarding when the car's trunk, doors, and windows opened and closed, when headlights turned on and off, and when gears changed or brakes were engaged.
- e. The main difference between the infotainment and telematics systems is that the infotainment system is about entertainment for the occupants of the vehicle, and



the telematics system is for collecting and reporting (transmitting) information—such as vehicle use data, maintenance requirements, and automotive servicing—about the vehicle. Typical telematics data may include turn-by-turn navigation, remote access, emergency calling, and maintenance notifications. Examples of vehicle telematics systems include General Motors’ OnStar, BMW’s “Assist,” and Mercedes’ “mbrace.” Some of these systems are integrated multimedia navigation and telematics systems in one (combined infotainment/telematics systems), like Toyota’s “Entune” and Ford’s “Sync.”

- f. The data generated, collected, transmitted, and retained by motor vehicles can provide valuable information in law enforcement investigations of crimes. For example, many infotainment systems support the importation of content and other data information from a particular user’s mobile device. Such data may include content that may provide attribution to particular user(s), including mobile device identifiers, wireless telephone numbers, user account details, passwords, user voice profiles, contact lists, call logs, text messages, pictures, e-mail, videos, web history, GPS coordinates, and other historical navigation information.
- g. I am aware that the computers (ECUs) within many motor vehicles store data for prolonged periods of time. Furthermore, even after a previously connected mobile device is removed from the physical vehicle, data may remain within the digital storage of the system. Such stored data can be used to identify locations, victims, witnesses, associates, and co-conspirators and may include communications and images of criminal activity. In sum, a forensic examination of a motor vehicle’s infotainment and telematics systems may reveal the vehicle’s GPS location

information, movements, operations, and user data at critical moments before, during, and after the commission of a crime.

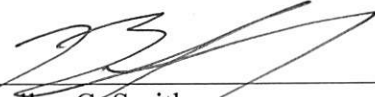
- h. As previously stated, the **SUBJECT VEHICLE** is a **Blue Tesla Model 3, Georgia license plate CVF5476**. I know from information obtained through the course of this investigation that Tesla Model 3 vehicles are equipped with the onboard data systems described above.
- i. The **SUBJECT VEHICLE** is currently being held by Hertz in anticipation of receiving legal process. To complete a forensic extraction, law enforcement may need to relocate the vehicle **to the FBI field office or other necessary facility (i.e. the FBI Laboratory)**.
- j. It may also be necessary, temporarily, to remove trim and other components of the Vehicle to access the information subject to search. It may also be necessary to repair the device, replace the screen, reconnect wires, and replace batteries. It may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes may include potentially destructive forensic techniques used to remove memory chips from computers and other electronic storage containers that may be found within the Vehicle. In the event that potentially destructive processes are required to perform this extraction, parts of the Vehicle may be destroyed and rendered useless.
- k. Furthermore, it may be necessary to return to the Vehicle and reconnect the infotainment and telematics systems to the Vehicle's power source to perform the extraction using forensic software. This is because there are various computer

networks working simultaneously when a vehicle is powered on, and in some vehicles, the infotainment and telematics systems require the other networks to work in tandem to complete the data extraction.

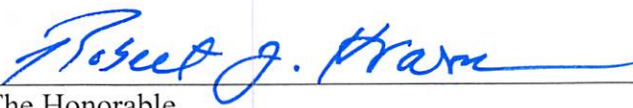
- I. The requested warrant authorizes a later review of the media and information seized or copied from the Vehicle, which review may continue past the date required for execution of the warrant.

### CONCLUSION

18. On the basis of my participation in this investigation and the information summarized above, I have probable cause to believe that the **SUBJECT VEHICLE** maintains evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 795 and 796. The items listed in Attachment B are evidence of these crimes, contraband, or fruits of these crimes, or property that is or has been used as instrumentalities to commit the foregoing offenses. Therefore, I respectfully request that a warrant be issued that authorizes the search of the **SUBJECT VEHICLE** described in Attachment A and the seizure of the electronically stored items listed in Attachment B.

  
\_\_\_\_\_  
Bradley C. Smith  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn before me on this 26<sup>th</sup> day of January 2024.

  
\_\_\_\_\_  
The Honorable  
United States Magistrate Judge